Competitive Strategies for Democracy in the Age of AI

Andrew Imbrie, Senior Fellow at the Center for Security and Emerging Technology at Georgetown University
June 30, 2020

Introduction

In a 1972 paper for the United States Air Force Project at RAND, the late Andrew Marshall defined what he called a more "efficient, effective U.S. competitive role."[1] His theory of the case was straightforward: The United States needed to sustain a long-term, strategic competition with the Soviet Union; the nature of that competition was poorly specified, but could be shaped in ways favorable to enduring U.S. advantages; and the United States should therefore assess the balance of strategic forces, clarify its goals, and develop competitive strategies to match its strengths against Soviet weaknesses.

The competition between the United States and China today is different from and far more complex than the U.S.-Soviet competition during the Cold War, notably in the levels of economic interdependence and the role of emerging technologies such as artificial intelligence. China, Russia, and other authoritarian powers seek to achieve strategic advantage through AI-enabled capabilities and systems.[2] By one estimate, more than 100 countries purchase surveillance and censorship gear from China and Russia, receive training on these technologies, or simply imitate methods of surveillance and censorship that are designed to control public opinion.[3] As the digital and physical environments become intertwined, authoritarian practices in one domain will increasingly encroach upon the other. At stake are the core values of liberty, equality, and justice that underpin free and open societies.

The novel coronavirus pandemic will accelerate these trends. Increased U.S.-China tensions, cascading economic crises, and renewed debates over the resilience of supply chains and the future of digital surveillance are all characteristics of a world that demands global cooperation but sorely lacks it. The fault lines between liberal democracies and illiberal, authoritarian regimes are widening at a time of growing turbulence in the

international system. Even before the virus, U.S.-China relations faced a heightened risk of conflict. The years ahead are likely to bring greater turmoil, with AI and other emerging technologies at the center of an extended, continuing strategic competition among the major powers.

In the long-term contest between the forces of democracy and autocracy, the United States should apply Marshall's counsel and develop more competitive strategies that play to its strengths. The right U.S. approach starts with its broad network of allies and partners. America has formed security guarantees with 52 countries in Europe, Asia, and Latin America, compared with Russia's five (Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Tajikistan) and China's one (North Korea).[4] The United States benefits from allies that share its values and produce strategic resources in AI, including computer and data science experts; private sectors that are innovative, dominant, and trend-setting; large and diverse pools data on which to train algorithms; governmental research and development (R&D) investments; diplomatic support for initiatives in AI safety and governance; and the clout needed to export norms and best practices internationally. In a world of globalized markets for AI talent and integrated supply chains, an alliance-centric strategy provides a competitive advantage over any single country that attempts to develop a robust AI ecosystem on its own.

A competitive strategy in AI will require the United States and its allies to assess their comparative advantages; identify anomalies and patterns in the strategic choices of authoritarian competitors that are deeply rooted; and match relative strengths against specific areas of weakness.[5] This paper focuses on the dynamics between the United States and China in AI. Based on an initial assessment of recent advances and long-term potential, it recommends that democratic nations sharpen their edge in five key areas:

- **Hardware edge**: exploit hardware chokepoints, leveraging the advantages that democratic nations have in the production of semiconductor manufacturing equipment and advanced AI chips.

- **Data edge**: develop common standards to share, pool, and store non-sensitive data sets around discrete projects, such as health intelligence and biosecurity, predictive maintenance, and maritime domain awareness; invest in privacy-preserving machine learning; and support research into new techniques for making personal data less relevant to AI systems, such as one-shot learning and advanced simulations.

- **Talent edge**: develop inter-allied human capital in AI, share best practices, and cultivate democratic networks of AI researchers through exchange programs, joint scholarships, and conference support, while ensuring research security among allies and partners.

- **Innovation edge**: harness the estimated two-thirds of global R&D that is conducted by democratic nations to foster collaboration in specific areas of promise, such as human-machine teaming methods and verification techniques for complex controls systems and AI-enabled, safety-critical infrastructure.

- **Rule-setting edge**: shape global norms and standards for AI, reflecting and supporting human rights and liberal values; create the conditions for a common AI market among democratic nations; and extend the benefits of AI to fragile democracies by establishing a multilateral digital infrastructure network.

Exploit Hardware Chokepoints

Integrated circuits (also called "chips") are China's top imports, valued at more than $312.7 billion per year.[6] China cannot meet its domestic demand of chips with indigenous production: 31.9 percent of its imports are shipped from neighboring Taiwan. Globally, more than 75 percent of the world's supply of chips are produced by companies based in the United States, Japan, Taiwan, and South Korea.[7] China produces older-generation chips in large quantities, but it is currently unable to manufacture leading-edge chips.

The United States should coordinate with allies and partners to target export controls at supply chain choke points that would increase the probability of maintaining China's dependence on AI chip imports. The United States should work with the Netherlands and Japan to control semiconductor manufacturing equipment, such as extreme ultraviolet lithography devices (EUV).[8] If these controls are successful and the major SME firms gain new buyers in democratic states to offset near-term revenue losses, the United States should coordinate with Taiwan and South Korea on end-use and end-user controls on the export of leading-edge AI chips to China.[9]

Share, Pool, and Safeguard Data

The conventional wisdom holds that "data is the new oil" and that "China is the Saudi Arabia of data."[10] A wiser U.S. approach is to recognize that AI remains highly context specific. The PRC's access to vast troves of data on Chinese purchasing habits may enable more targeted applications for Chinese businesses, but this data does not necessarily confer an advantage in the military sphere. In addition, Beijing faces bureaucratic obstacles and institutional constraints on accessing consumer data, as evidenced by its growing concerns over "information islands" that inhibit the sharing of large government datasets.[11]

The United States benefits from an array of remote military sensors and collection platforms with global reach. These platforms generate more data, in more locations, with greater precision than comparable platforms of near-peer competitors. Beyond the quantity of data, the quality and diversity of data are important determinants of its value for AI. The most valuable U.S. tech companies gain the bulk of their revenue outside the United States; by contrast, Chinese tech firms gain nearly all of their revenue from the Chinese market.[12] America also benefits from greater cloud storage capacity, widespread use of business analytics software, and access to business-specific data, which can be valuable for training machine learning systems.

The United States should match its relative strengths on data to Chinese weaknesses in three areas:

- First, the United States can offset any potential data advantage China might have by deepening cooperation with allies and partners to develop common standards for sharing, pooling, and storing non-sensitive data sets. These projects could start small, such as collaboration on predictive maintenance or maritime domain awareness. The Departments of State and Commerce and the National Institute of Standards and Technology should work with counterparts in allied and partner countries to formulate common data archival procedures and protocols for sharing models and data sets.

- Second, the United States should heighten the contrast with China's approach to data collection by creating an accelerator fund for privacy-preserving machine learning with like-minded countries. By coordinating investment initiatives in homomorphic encryption, secure multiparty computation, and federated learning, America and its allies could perform analysis on larger, more diverse pools of data without compromising the privacy of individuals and organizations whose data are in the pools.[13]

- Third, the United States should exploit China's reliance on large quantities of data by pursuing investments into new techniques for making personal data less relevant to AI systems. The Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF), and other relevant government agencies should deepen partnerships with industry and academia to support research into advanced simulations and improvements in transfer learning. Advances in one-shot or few-shot learning may enable AI systems to improve their performance and generate more accurate inferences with smaller data sets.[14]

Develop Inter-Allied Human Capital for AI

China faces a number of deficits in its drive to attract and retain talent in AI. One study estimates China's AI talent pool at 18,232 individuals compared with 28,536 individuals in the United States.[15] The disparities are even greater for "top" AI talent. According to the H-Index, China boasts less than a thousand individuals in this category relative to 5,518 top AI researchers in the United States.[16] President Xi Jinping has made it a priority to strengthen China's domestic S&T ecosystem and attract overseas Chinese and foreign talent. The results are mixed.[17] China has rapidly developed its domestic science and technology capabilities and modernized education at the undergraduate and graduate levels. Nevertheless, China struggles to attract overseas Chinese and foreign talent. The Center for Security and Emerging Technology tracked the professional histories of 1,999 AI PhD graduates of top U.S. universities between 2014 and 2019 and found consistently high stay rates among international graduates. According to the data, "Around 90 percent of international AI PhD students take a job in the United States after graduating, and more than 80 percent stay in the country for at least five years…Stay rates are highest—exceeding 90 percent—among students from Taiwan, India, Iran, and China, and lower—around 75 percent—among students from European countries."[18]

America's openness and diversity are sources of enduring strength. The United States draws AI researchers with its world-class universities and companies, higher standards of living, relatively higher compensation, and commitment to human rights, liberty, and equality. The majority of computer scientists and electrical engineers employed in the United States are foreign-born, and the figure rises to roughly two-thirds of those employed in Silicon Valley. As for the future AI workforce, more than two-thirds of graduate students in computer science and electrical engineering are foreign-born, while the domestic pool of AI graduate students has remained relatively flat since the early 1990s.[19]

By remaining open to foreign talent and cultivating international networks of researchers through exchange programs with democratic allies and partners, the United States can widen the gap with China in a critical area of AI development. To further this effort, the U.S. government should commit resources to hosting and convening workshops among AI researchers from democratic countries and deepen partnerships with existing networks, such as the Confederation of Laboratories for Artificial Intelligence Research in Europe. Additional programs, joint scholarships, and conference support could synchronize efforts to grow the pool of AI talent. The United States and its allies should coordinate with the private sector on job placement and training programs, including hosting recruiting sessions that bring together representatives from government, industry, and academia.

Launch an AI R&D Collaboration Challenge

America still leads the world in R&D spending, but China is closing the gap. U.S. federal spending on R&D as a percentage of GDP has declined by more than half from its Cold War heights. Meanwhile, China has increased its R&D spending 30-fold since the early 1990s. The networks critical to the success of American innovation have frayed as the federal government retreats from its traditional role as an engine of scientific progress. If not reversed, these trends could undermine the strength of U.S. R&D in emerging technologies.

The United States should increase total U.S. R&D funding to three percent of GDP and devise strategies for engaging the primary sources of R&D funding and implementation, including the federal government, industry, philanthropy, and academia. The United States can balance China's advantages of scale by linking arms with democratic allies and partners. An estimated 65 percent of the world's most promising start-ups are located in the United States, and 28 percent are located in allied and partner countries.[20] Together, the United States and its allies account for nearly two-thirds of global R&D spending, including public and private R&D investment.[21]

Democratic nations should leverage this pool of R&D and deploy it in areas that will enable them to develop economically, innovate collaboratively, and strengthen liberal values.

When the NSF or DARPA fund AI research, they put out calls in specific subfields or functions of AI. The U.S. government should expand coordination with foreign science funding organizations to solicit research on complementary agendas, such as human-machine teaming methods and verification techniques for AI-enabled network control systems for power generation, dams, and other safety-critical infrastructure. Annual meetings of performers could provide a forum for collaboration on future calls or the identification of common agendas among allied research communities. For example, the AI4EU test bed is an EU initiative to pool government resources from many countries and fund AI researchers. The United States and its allies should explore such innovative models with countries in Europe and elsewhere.

Shape Global Norms and Standards for AI

China has ramped up its engagement in international bodies to define the standards for mobile network technologies and the future governance of AI. The United States and its allies face risks and opportunities. On the one hand, standard-setting could become the casualty of geopolitical competition as leading countries precipitate a race to the bottom. On the other hand, China already asserts its principles and standards through a variety of multilateral fora. The United States and its allies should act now to set global standards for AI that reflect democratic values, while addressing critical questions surrounding the rollout of 5G, facial recognition for surveillance, automated cyber exploitation and defense, and autonomous weapons systems.

One of the United States' comparative advantages has been to write the rules of the road for international relations. America should leverage its diplomatic capacity, hard-won experience, and broad relationships to shape the architecture in which AI technologies are developed and deployed. To this end, the United States will have to lead a multilateral initiative with allies and partners to set international rules of conduct for AI. This effort could build on and extend the OECD Principles on AI and the International Organization for Standardization working group initiatives on standards for data and AI safety and security. Longer term, the United States and its allies should lay out the conditions for a common AI market, including standards for testing, evaluation, verification, and validation of AI technologies, as well as common practices for certifying companies that support liberal democratic values and privacy. This common market would create incentives for democratic countries and leading firms to abide by shared principles in the development and deployment of safe and reliable AI.

When it comes to stimulating innovation among democratic nations, the United States and its allies should not mimic China's model of state-driven, top-down national development strategies that trade investment for market access. The costs of this approach are already apparent in the wake of COVID-19: China's sprawling investments in its Belt Road Initiative are becoming liabilities as countries in the developing world buckle under the economic strains and sue for debt relief. Washington can best advance its interests and values by launching a multilateral digital infrastructure network to ensure that digital systems in emerging markets are open, secure, resilient, and interoperable. As part of this effort, the United States and its allies should integrate federated learning techniques and data privacy into digital capacity building efforts with developing countries. By creating an accelerator fund for privacy-preserving machine learning technologies, the United States and its allies could promote an alternative model of development that puts data protection and privacy at the absolute center.

Blend Strategic Approaches

Developing more competitive strategies in AI will require blending two strategic approaches: signaling and shaping.[22] Signaling is about leveraging alliance commitments, mobilizing resources, and reforming institutions to gain the upper hand in today's competition. Shaping is about setting the rules of the road in the competition for the future. The United States can signal resolve to strategic competitors and reassurance to allies and partners with smart investments and clarity of purpose. Equally important, the United States will need to deepen cooperation with allies and partners to shape the ecosystems for development and deployment of safe and reliable AI. By exploiting hardware chokepoints, investing in privacy-preserving machine learning, sharing non-sensitive data sets, fostering R&D collaboration, developing human capital, promoting global norms and standards in multilateral fora, and establishing a digital infrastructure network, democratic nations can shape the global environment in ways that advance their interests and values. The stakes are clear, and the stage is set for the United States and its allies to rise to the challenge.

Acknowledgements

Endnotes

1. A.W. Marshall, *Long-Term Competition with the Soviets: A Framework for Strategic Analysis (U)* (Santa Monica: RAND Corporation, 1972).

2. See, e.g., Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism," *Brookings Institution*, August 26, 2019; Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," *Centre for Technology and Global Affairs*, University of Oxford, September 17, 2019; Kara Frederick, Daniel Kliman, and Ely Ratner, "The Low Road: Charting China's Digital Expansion," *Center for a New American Security*, September 4, 2019.

3. Weber, "The Worldwide Web of Chinese and Russian Information Controls."

4. Estimates of the number of U.S. allies vary depending on whether one includes formal, mutual defense treaty commitments, non-treaty relationships, defense partnerships, and other strategic alignments. The author's estimate of 52 U.S. allies is based on the State Department's list of "U.S. Collective Defense Agreements." For other estimates and definitions, see Mira Rapp-Hooper, *Shields of the Republic: The Triumph and Peril of America's Alliances* (Cambridge: Harvard University Press, 2020); Michael Beckley, "The Myth of Entangling Alliances," *International Security* 39, no. 4, (Spring 2015): 7-48; and Adam Taylor, "Map: The U.S. is bound by treaties to defend a quarter of humanity," *Washington Post*, May 30, 2015. It is worth noting that measures of formal security guarantees do not capture the bourgeoning China-Russia relationship or China's expanding science and technology partnerships through the Belt and Road Initiative.

5. On the requirements of competitive strategies, see Octavian Manea, "The Art of Tailoring Competitive Strategies," *Small Wars Journal*, March 26, 2014. For more on how the United States can compete effectively in AI, see Tim Hwang, "Shaping the Terrain of AI Competition," *Center for Security and Emerging Technology*, June 2020.

6. UN Comtrade database. On China's top imports, see Daniel Workman, "China's Top 10 Import," *World's Top Exports*, May 5, 2020.

7. UN Comtrade database; SEMI, World Fab Forecast, May 2019 edition.

8. Saif M. Khan, "Maintaining the AI Chip Competitive Advantage of the United States and its Allies," *Center for Security and Emerging Technology*, December 2019.

9. Saif M. Khan and Carrick Flynn, "Maintaining China's Dependence on Democracies for Advanced Computing," *Brookings Institution*, April 2020.

10. See, e.g., "The World's Most Valuable Resource is not oil, but data," *The Economist*, May 6, 2017; Kai-fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (New York: Houghton Mifflin Harcourt, 2018).

11. Andrew Imbrie, "Artificial Intelligence Meets Bureaucratic Politics," *War on the Rocks*, August 2019.

12. Based on analysis of monthly user data of most valuable U.S. and Chinese tech companies.

13. On privacy-preserving machine learning, see Roxanne Heston and Helen Toner, "Have Your Data and Use it Too: A Federal Initiative for Protecting Privacy While Advancing AI," *Day One Project*, January 23, 2020.

14. See, e.g., Hwang, "Shaping the Terrain of AI Competition"; Li Fei-Fei, Rob Fergus, and Pietro Perona, "One-Shot Learning of Object Categories," *IEEE Transactions on Pattern Analysis and Machine Intelligence* 28, no. 4 (April 2006): 594-611.

15. "China AI Development Report 2018," *China Institute for Science and Technology Policy*, Tsinghua University, July 2018.

16. "China AI Development Report 2018," Tsinghua University, July 2018.

17. Remco Zwetsloot, "China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response," *Brookings Institution*, April 2020.

18. Remco Zwetsloot (lead author), James Dunham, Zachary Arnold, and Tina Huang, "Keeping Top AI Talent in the United States," *Center for Security and Emerging Technology*, December 2019, iv. See also Remco

Zwetsloot, Jacob Feldgoise, and James Dunham, "Trends in U.S. Intention-to-Stay Rates of International Ph.D. Graduates Across Nationality and STEM Fields," *Center for Security and Emerging Technology*, April 2020.

19. See, e.g., Zwetsloot, Dunham, Arnold, and Huang, "Keeping Top AI Talent in the United States"; Remco Zwetsloot, Roxanne Heston, and Zachary Arnold, "Strengthening the U.S. AI Workforce: A Policy and Research Agenda," *Center for Security and Emerging Technology*, September 2019.

20. Susan Decker, "Majority of Promising AI Startups Based in US," *Bloomberg*, March 3, 2020.

21. Melissa Flagg, "America's Future Lies in Technical Alliances," *Center for Security and Emerging Technology* (blog), January 8, 2020; Melissa Flagg, "Global R&D and a New Era of Alliances," *Center for Security and Emerging Technology*, June 2020.

22. On signaling and shaping in the cyber context, see Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020).